The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

STRATEGY
RESEARCH
PROJECT

DEFENSIVE INFORMATION WARFARE IN TODAY'S JOINT OPERATIONS: WHAT'S THE REAL THREAT?

BY

LIEUTENANT COLONEL BRUCE W. ASHMAN
United States Army Reserve

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1997

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

DEFENSIVE INFORMATION WARFARE IN TODAY'S JOINT OPERATIONS: WHAT'S THE REAL THREAT?

by

LTC Bruce W. Ashman

Colonel (Ret) Michael Morin
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any or its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. ARMY WAR COLLEGE,
CARLISLE BARRACKS, Pennsylvania 17013

ABSTRACT

AUTHOR: Bruce W. Ashman (LTC), USAR

TITLE: **Defensive Information Warfare in Today's Joint Operations: What's the Real Threat?**

FORMAT: Strategy Research Project

DATE: 7 April 1997 PAGES: 40 CLASSIFICATION: Unclassified

Information warfare (IW) is an emerging concept that affects the use of automated systems and reflects the growing realization that information technology can be used to gain an advantage over other users. Since the Gulf War, the incidents of information systems attacks have increased, especially in the civilian environment. Attacks against military systems have gone as far as penetrating sensitive, previously secure systems. As this threat against information- or computer-based systems becomes more blatant, it raises the question of how vulnerable to attack are our automated military systems. Emerging technologies promise greater speed, accuracy and reliability for military operations while simultaneously producing greater lethality and situation awareness. However, as the Armed Forces depend more and more on these systems to perform routine and specialized

operations, the risk of penetration, disruption, or even compromise becomes apparent. While information warfare has great potential as a valid offensive tool, this paper explores the threat to unified and joint military operations from a defensive information warfare perspective. We must first identify what the threat entails and design defensive procedures because this is where the greatest vulnerabilities lie. Research and development of IW as an offensive weapon can be pursued and funded along with other conventional weapons programs. What is critical is identifying weaknesses and correcting them before we become victims of information warfare itself.

TABLE OF CONTENTS

Introduction

The Information Age is upon us and will take us into the Twentieth Century and beyond. One of the strongest and most pervasive indicators of this is the innovative way people are using information technology.

As a stark example, during the Persian Gulf War teenage Dutch hackers (computer systems attackers) penetrated Department of Defense (DoD) computer systems 34 times. Although most of the breaches occurred in Internet connections and involved sensitive rather than classified information, the hackers were able to move about freely within the systems and remained undetected. From their home base they were able to change software to allow subsequent access, altered then reproduced military information, and even stored stolen information at university sites in the United States.[1]

Commercially, in 1995 a Russian graduate student in St. Petersburg broke into New York's Citicorp computerized cash-management system over 40 times. He used the bank's automated cash transfer process to move more than $12 million to banks worldwide and at one point had access to Citicorp's $500 billion holdings,[2] before he police caught him.

Further, in March of this year, the Army's National Training Center (NTC) at Fort Irwin, California will host a major experiment involving a unique force. This force, a Brigade-size element of the 4th Infantry Division called the EXFOR (for Experimental Force), will be equipped with the latest in digitized technology. Virtually all of its vehicles will have some combination of the Single Channel Ground and Airborne Radio System (SINCGARS), the Enhanced Position Location Reporting System (EPLRS), the Battlefield Combat Identification System (BCIS), the Portable Lightweight Unit Global Positioning System Receiver (PLGR), and the Force XXI Battle Command for Brigade and Below (FBCB2).[3] These systems totally automate the organic communications capability of the Brigade and represent a major investment of the Army in digitization.

These accomplishments are evidence both of the increasing dependence on automated systems and the concomitant vulnerabilities associated with those systems. Information technologies have spawned a new, potentially dangerous use: information warfare (IW). But is the so-called information warfare phenomenon a unique occurrence or just a passing fad? Does it represent a viable threat to all information-based systems? Even more important, is the Joint Community depending too much on the integration of computer- and information-based technology to perform its primary functions, thereby opening itself up to potentially catastrophic disruption from Information Warfare attacks? Finally, while research and development of offensive IW techniques are certainly worth pursuing, defensive IW must take priority. It is here that the greater risk lies, not in developing another tool for the warfighters conventional weapons kit bag. This paper, then, looks at the threat to Joint information-based systems as planners invest more and more in technology to conduct unified, joint, multinational and interagency operations. The threat to information-based systems is valid and it affects how planning for these types of operations is conducted and executed.

What is Information Warfare?

The effort to define information warfare is evolving. In his 1995 work on the subject,[4] Martin Libicki offers seven forms of IW. These are: command and control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare, economic information warfare (EIW), and cyberwarfare.[5] Several of the terms, such as EW and PSYW have been used since at least World War II. What is new is that the terms differentiate the ways one can use information-based platforms for one's advantage. For instance, electronic warfare refers to both radioelectronic and cryptographic techniques, such as antiradar and anticommunications, or operations aimed at disrupting, destroying or interrupting someone's communications systems. Hacker warfare, on the other hand, refers primarily to attacks on computer-based systems. Libicki's work is important because the author makes the key point that "information warfare, as a *separate* technique of waging war, does not exist."[6] He suggests that in combination with other conventional forms of combat information warfare can have its most effective use. This is especially true of offensive information warfare. However, Libicki also discounts certain types of warfare, for example, hackers, as a threat to national security.[7]

The Defense Department has been wrestling with the terminology of the Information Age at least since the early 90's. Because technology in the IW field is developing so rapidly, it is difficult to settle on agreed-upon definitions that serve to describe IW aspects before they change. For instance, DoD Directive S-3600.1, Information Operations (IO), added at least eight new unclassified terms between the 1992 publication and the 9 Dec 96 version of Information Operations. They include:

Computer Network Attack (CN), Information Assurance, Information Environment, Information Operations, Information Superiority, Information System, Information Warfare, and Special Information Operations. These represent a growing sophistication with information warfare techniques and the realization by the Defense Department that information warfare -- in the broadest sense -- has the potential for military application.

Because information is so rapidly evolving, then, the attempt to accurately define aspects associated with this phenomenon is becoming more sophisticated, as stated above. Some would argue that definitions in the IW arena are meaningless.[8] However, in order to focus on the threat of information warfare, it is necessary to establish a start point.

In the military arena[9] Joint Publication 3-13.1, Joint Doctrine For Command and Control Warfare (C2W), information warfare is defined as: "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own" similar systems.[10]

This definition does several things. First, it points out that there *are* actions that one can take to gain an information advantage over some other information system user. Second, and conversely, there are also actions that one can take to defend his own systems. Third, there is a recognition (at least in the Joint arena) that people can use information and information systems as warfare. Fourth and from a military perspective, there are both offensive and defensive aspects to information warfare. This means that information warfare may be a military instrument of power which warfighters must consider and both defend against and incorporate in their warfighting "kit bag."

Offensive information warfare, although publications do not officially recognize it as such, is the first half of the Joint definition. Defensive IW, the second half of the definition, is defending our own systems against intrusions, disruptions, denials of service or other misuse of our systems for other than the intended purposes. For the purposes of this paper, I will concentrate on defensive information warfare. What is important to understand, however, is that concepts of IW and offensive -- defensive capabilities are currently in transition. Also, as technology and applications become more sophisticated, so too will the attempts to grasp information technology's full potential metamorphose over time.

Nevertheless, in order to determine what information warfare means we first have to look at the environment that has spawned this phenomenon.

The Information Warfare Environment

It is difficult at best to determine an exact date when the so-called Information Age began. It may have begun when Man first began to write history. It might have started with the invention of the printing press, the telegraph and telephone, or even with the invention of the microprocessor twenty-five years ago. Suffice it to say that the last quarter of this century has seen a literal explosion in the use of information technology worldwide.

With the discovery that the microprocessor or computer chip could store, process, and transfer information as data or bitstreams faster, more accurately, in larger quantities, and more reliably than manual or paper processes, came the realization that this ability had vast potential for information processing. As shown in figure 1, however, as we use more and more information technology, the broad base that supported the Industrial Age from which we came, is drastically reduced. What figure 1 dramatically illustrates is not only the focus on information technology but, figuratively, the precarious balance that seems to emanate from dependence on that technology.

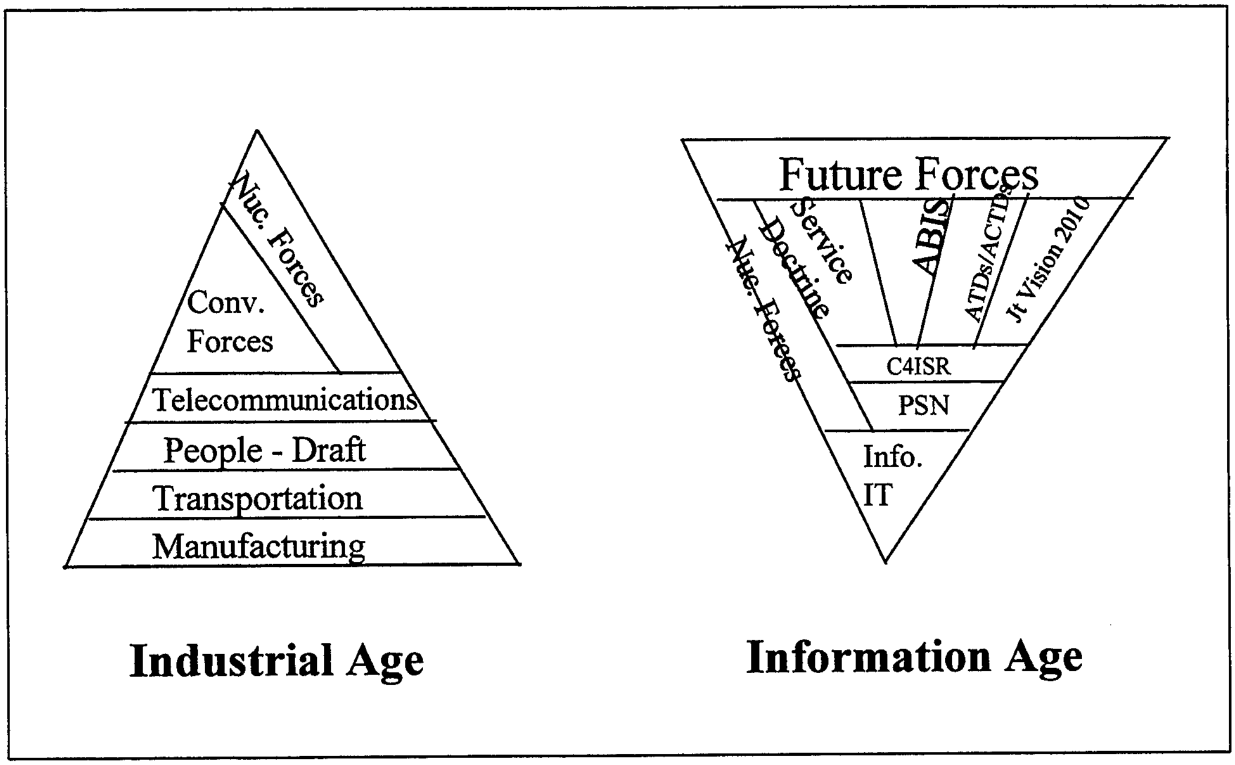

Figure 1

Conv. Forces= Conventional, nonnuclear forces ABIS= Army Battlefield Information System, Nuc. Forces= Nuclear forces ATDs/ACTDs= Advanced Technology Demonstrations/Advanced Concepts Technology Demonstrations Jt. Vision 2010= (The Joint Chiefs of Staff) Joint Vision 2010 C4ISR= Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance PSN= Public or Packet Switched Network Info IT= Information and Information Technology[11]

Within this Information Age environment are initiatives to interconnect individual processes to form more efficient infrastructures. Systems such as the Global Information Infrastructure (GII), the National (U.S.) Information Infrastructure (NII), and the Defense (U.S. DoD) Information Infrastructure, seek to make it easier to do routine processes and conduct business more quickly, accurately, and conveniently. (See *Draft* Joint Publication 3-13, Joint Doctrine For Information Operations, 21 Jan 97 for a discussion of how these levels of infrastructure interrelate to form the IO hierarchy.) As a commercial application, if a person has bills to pay which require writing checks to several locations, being connected to those locations by means that allow the electronic transfer of funds has its advantages. The person could potentially conduct all those transactions on a home computer, with the appropriate software, and a modem. Computer-based technology is easing the lives of millions of consumers through such convenient use of technology. It is easy and relatively inexpensive to obtain this capability.

The Internet and World Wide Web are other examples of information-based systems that are becoming quantitatively more proficient modes of information transfer for increasing numbers of people worldwide. The Wall Street Journal, in October 1996 reported that the number of U.S. households linked to the Internet during the past year doubled to 14.7 million.[12]

Electronic mail (E-mail) is another recent capability that is becoming increasingly popular as a means of instant communications. The German magazine Stern predicted that E-mail "will continue to be the dominant activity on the Internet into the next century." It predicted the number of E-mail users would grow to 200 million by the year 2000.[13]

As an example of how information technology has spread, Chart 1 lists just a small sampling of the many military systems being fielded in the Joint arena.

CHART 1: Current and Projected Joint Computer-Based Systems

ISR
(Sense/Find)

AWACS
Rivet Joint
EP-3E
JSTARS
ES-3A
SBIR
Tier 2(+)
Tier 3(-)
U-2
TARPS/ATARS
MTI
Hunter
REMBAS
Magic Lantern
ISAR
NVG
FDS
JDISS
etc.

C4I
(Decide/Direct)

GCCS
MILSTAR
JSIPS
DISN
SABER
C4I FTW
TIES
TADIL J
TRAP
TACSAT
MIDS
STEP
SONET
JMCIS
Link-16
DMS
JTIDS
JDSS
etc.

Precision Force
(Fight/Destroy)

SFW
JSOW
TLAM (BLK III)
ATACS/BAT
THAAD
SLAM
CALCM
JDAM
Have Nap
AGM-130
HARM
TLAM (BLK IV)
A-Hawk
Hellfire II
Javelin
LOSAT
Long Bow
SADARM
AFTADS
etc.

ISR= Intelligence, Surveillance, Reconnaissance systems   **C4I**= Command, Control, Communications, Computers, and Intelligence systems[14]

The purpose of incorporating this technology in so many of the military's processes is to gain, in the words of the Chairman of the Joint Chiefs of Staff, "full-spectrum dominance" of the battlefield.[15] As the Information Age has shown, developing technologies can add speed, reliability, accuracy, locations, simultaneity and depth to any military system that can be automated.

The advantages of advanced technologies for U.S. military forces are that they allow warfighters to gain information about a physical battlefield, about the geography, weather, opposing forces, friendly forces; to communicate near real-time to real-time information in a variety of redundant, reliable means; to transfer that information to anywhere on the battlefield the commander wants; to use that information to create extremely accurate targeting for weapons systems; to then guide precision weapons and maneuver forces to targets with minimal collateral damage; and to deliver logistics in timely, economical ways to support the warfighter. More importantly, as the National Defense University's Strategic Assessment 1996 notes: "The U.S. military's advantage in applying information technology to warfare does not derive from special access to this technology but from competence at systems integration."[16] Unfortunately, integration, not security seems to be the goal of joint interoperability initiatives.

Since the end of the Cold War, the U.S. military is moving from a threat-based force (formerly facing the Soviet Union) to a capabilities-based force. The philosophy is that with the uncertainties of the near future and the absence of a single major "peer competitor," the U.S. must be prepared to face a variety of challenges in many forms. The ability to harness the vast potential of technology, and information technology in particular, is one of the reasons the U.S. remains the only superpower. Commenting on the current Quadrennial Defense Review (QDR), COL Jim Dubrik notes: "America can bring to bear significant technological advantage to its conventional forces, and it should. Ground maneuver forces, artillery, helicopters, surface missiles, fixed-wing aircraft, surface vessels, and submarines -- all can be connected via information technologies."[17]

Another advantage of integrating Information Age technology into military operations is that we can improve interoperability between the separate services. If the U.S. military is going to operate "jointly" in future operations (from combat to operations other than combat), interoperability has to improve on the success achieved during Operation Desert Storm. By using the same inter-connected systems, such as the Global Command and Control System (GCCS), with standardized protocols and software, and by fielding such systems to key decision-makers in theaters of operation, interoperability will be improved. Incidents of friendly fire and fratricide will decrease as users (of those information systems) will have the same "picture" of the battlefield, the same situational awareness.

The Persian Gulf War is only the beginning of the power that information technology can have on the battlefield. As an illustration, in that war information warfare (by U.S. forces) meant knocking out key communications nodes. By striking Sadam Hussein's command and control centers -- his eyes and ears of battle -- Iraqi troops were cut off from command and intelligence sources and were left paralyzed against U.S. combat forces.[18] As former Army Material Command (AMC) Commander General Jimmy Ross put it, "Iraq lost the war before it even began."[19]

Further, the ability to provide larger amounts of and more accurate, more timely information to friendly forces during combat will allow U.S. forces to decide quicker than the enemy; to mass fires simultaneously, more accurately, and in depth; to react quicker and more intelligently to possible enemy moves; and thus, to get inside the enemy's decision cycle to defeat him. Alan D. Campden, author of *The First Information War*, wrote of the success that accurate information and information technology had in Desert Storm. "Knowledge came to rival weapons and tactics in importance," he said, "giving credence to the notion that an enemy might be brought to its knees principally through destruction and disruption of the means for command and control."[20] Truly, information technology can bring accurate, decisive power to the battlefield.

In a climate of geometrically advancing technology, then, with a seemingly endless potential to the use of technology backed by American scientific knowledge and industry: what is the problem with the use of technology? What, if any, are the vulnerabilities and the risks associated with using it? Why is it even worth looking at these?

The Risks Associated With Information Technology

We can group these risks into four general categories: dependence on information systems, adversarial information attacks, the nature of information itself, and natural or man-made disruption.

First, as a tool of the Information Age, information technology is extremely useful, convenient, economical, and as shown above, when used with intelligence (in the non-military sense) it can have tremendous advantages for the user. How we use it, however, may entail some of information technology's greatest faults. For one, as technology matures, the products become more affordable, allowing more people to obtain and use the "technological advantage" that ownership brings over non-automated processes. Almost anyone who has the money can own increasingly more powerful computers, whether those users are American, French, Iraqi, North Korean, Brazilian, or Russian. A computer does not recognize the intent, nationality, purpose, relationship to the United States, or potential use of the computer. Information technology is becoming ubiquitous. There are also no known legal restrictions to the general sale of computers in the United States. Ownership now can include -- for a price -- access to open sources of information.

Fielding policies currently in vogue in the Department of Defense encourage proliferation of computer technology. As noted previously, the EXFOR has spent almost three years equipping its Brigade-plus of vehicles and personnel with the latest information technology in an attempt to maximize the information advantage. Key military leaders, additionally, support the integration of information technology.[21] But are we automating too much? Are we putting all our eggs in the automation basket? General Ross puts it more succinctly: "The rapid deployment and synchronization of forces, the gathering of timely intelligence and the maintenance of a fast tempo of operations are all dependent on the transmission of accurate and timely information."[22] The danger is that each user -- which indicates in itself his or her importance to the future battle -- must have the latest battlefield information (on a battlefield that is dominated by information advantage). The consequence is that if a critical element of that user's situational awareness picture is missing, it may cause that user to take some unexpected (and unwanted?) action. The need to have a complete picture absolutely mandates perfect information flow. We have thus programmed infallibility into our expectations of information technology. In the often-heard lament of Signal officers, heightened expectations of perfect communications in exercises and in real operations, leads to planning for "assured communications," which in the Information Age becomes assumed communications.

Another associated weakness of information systems is that too often there is the creation of a so-called single point of failure somewhere in the system or infrastructure supporting the system. As an example, the Global Positioning System (GPS), a satellite-based worldwide location system, allows a commander at any level to theoretically know where any of his subordinate elements (also equipped with GPS) is, anywhere on the battlefield. U.S. forces in Desert Storm used the system extensively. It was so successful and American units relied on it to such an extent that if and when the system became inoperable, soldiers were unable to remember how to use other location devices, such as the hand-held lensatic compass.[23] So dependent are U.S. forces becoming on GPS for a whole range of systems from target acquisition to logistics, that the potential for disaster is apparent. At a recent Army War College seminar on the Army After Next, the idea surfaced of shooting down the satellites on which the system is based, as the first shot in some theoretical future war. This would have the effect of rendering the GPS-based systems that the military is investing so heavily in, virtually useless.

A second risk associated with information systems is their vulnerability to attack. Although there is some agreement as to what constitutes an information attack[24] there is no doubt that attacks are occurring and at an increasing rate. The Defense Information Systems Agency (DISA), charged with collecting data on such attacks on DoD systems, reported that since 1992 there have been over 38,000 attacks. Of these attacks, 65% were successful. Further, of these successful attacks only 4% were detected and only 267 of these were reported.[25] What is remarkable is that these attacks were on Defense systems that are afforded the added protection, so to speak, of being inaccessible to public scrutiny. How extensive is the actual threat from attack? The former Director of Central Intelligence, John M. Deutch, claims that "the degree of computer-based 'cyber' attacks is second only to that posed by nuclear arms and other weapons of mass destruction."[26] In a warning to Congress about the dangers of information attacks, Deutch opined that, "the electron is the ultimate precision-guided weapon."[27]

Admittedly, the United States is a tempting target for information attacks. The Internet, which freely crosses military as well as commercial telecommunications systems, is a valuable open source for information. This is rarely, if ever classified or even sensitive information. However, it is increasingly a valuable and easy-to-use source of detailed directions how to use a plethora of America's best software products and it has access to a wide variety of databases. Why not? The Internet was designed to increase the networking capability of database systems, to allow user-friendly access, and it is spreading worldwide. The U.S. is also technology-rich, especially in information technology. Organizations or single users who can gain access to American information systems and who can become superusers (that is, able to control access to various parts of the system) are potentially limited only by their own resources and initiative. So far, however, none of the hackings that have been detected have indicated any conspiratorial connection, organized pattern, or concerted threat.

But how long can this "passive" defense hold? The American people once thought themselves isolated from terrorist attacks on this continent until the World Trade Center and Oklahoma City bombings. Can we afford to be complacent about information attacks that have, after all, not claimed any lives? The danger is not in any information attack's "lethality," but what it portends about information systems and the information that travels along those paths.

The third risk has to do with the very nature of information. What the Information Age has produced is a heightened awareness that information is power. But what is important for national security and strategic planners is having the *right* information, at the *right* time and in the *right* place.

To an adversary, any bitstream of information can potentially be or become a bitstream of intelligence. In military operations, planners usually discern operational trends after long periods of monitoring an adversary. Individual bits of intelligence, gained over time, potentially form into a picture. An adept information system intruder can be anything from a passive "listener" (undetectable unless you are aware he is listening) to an active disrupter.

Further, the information realm itself is borderless: it knows no national boundaries. Information is not constrained by time or space, by law or regulation. "Information is fluid," says Professor George F. Stein.[28] It is not subject to physical restrictions, except the limitations of the information systems which carry it. Examples of such restrictions are trunk capacity, satellite accessibility, compatibility of equipment, and software protocols. It is also extremely difficult to trace or identify an attacker once he has turned off his system. Information flow stops when one turns off the electricity.

The fourth risk associated with information systems is disruptions from natural or man-made causes. Though these are infrequent, certain aspects may be self-induced.

For instance, according to the Defense Science Board's Task Force on Information Warfare -- Defense, the national information infrastructure is heavily dependent on commercial services, such as power and natural gas systems.[29] Barry Horton, principal Deputy Assistant Secretary of Defense states that fully "95 percent of military communications are over commercial networks."[30] Many U.S. military installations depend on local commercial gas and power lines as their primary energy resource. The degree of military control over these external systems is potentially degraded in times of catastrophic outages. It is imperative that installations have effective back-up systems for critical information-based systems. Also, redundancies in cabling and in routing systems are effective protective measures.

In developing defensive measures against IW outages, we should be asking the following questions: What key systems are likely targets of attack? What critical infrastructures, such as power sources and transmission lines, should be protected? What redundant infrastructure capabilities need to be engineered? What constitutes an IW "attack"? How do users of military information systems (and potential targets of IW attacks) train for, recognize, and report attacks? Developing strategies to counter this potential disruption at the lowest level of operations will help to ensure systems remain operational.

One of the potentially most damaging weapons to be used against U.S. information systems is the virus. These destructive engines are simply programmable codes that when introduced into a computer system, alter the operation of the system itself. Viruses, known by such unique names as "Michelangelo," the "Morris Worm," and "Meatgrinder," can cause permanent or temporary damage or disruption to a computer's storage media and memory areas. The danger of viruses is that any computer system (military or civilian) is susceptible to a virus attack. They usually target certain hardwares and are therefore effective, unanticipated and usually undetected until they have been executed. Lastly, viruses are programs; that is, they are man-made and not naturally occurring in computer systems. They are therefore created for a purpose, exclusively injurious to information systems. Most importantly though, there have so far been no efforts to outlaw viruses, due to their relatively recent appearance on the scene.

What is the potential for using a virus as a weapon? Two of the leading authorities on viruses, Paul Evancoe and Mark Bentley, claim that, "The possibility for the employment of CVW

[Computer Virus as a Weapon] [is] only limited by the imagination. The technology and genius required to develop such powerful viruses," they state, "exists now."[31]

We have looked at information warfare, the current commercial and military environments of the Information Age, some of the vulnerabilities and risks associated with the use of information technologies, and a few of the instances of actual IW attacks. It is now time to turn to the threat to current information systems, and particularly Joint systems.

What is the Information Warfare Threat to U.S. Joint Systems?

The overall threat derives from four sources: the absence of a coherent national security policy to combat IW, the nature of U.S. society in the Information Age, the Information Age environment itself, and the absence of a significant external conventional weapon threat.

Any national security policy to combat IW attacks must start at the top. President Clinton's current statement on national security strategy,[32] stresses the intent to protect American society through a strategy of active engagement in world politics, keyed to the enlargement of the pool of democratic and open-market societies. However, it pays scant attention to information warfare.[33]

Although a straightforward information warfare declaration is not part of the National Security Strategy, at least at this time, other important processes address related information systems issues. Two of these are the Critical Infrastructures Working Group (CIWG) and the President's National Security Telecommunications Advisory Committee (NTSAC).[34]

Derived from the National Security Strategy and similarly focused, the National Military Strategy published in 1995,[35] calls "winning the information war" one sub-component of the "fight and win" element of the strategy. It recognizes that we can gain leverage by obtaining information systems technologies but it stops short of defining a specific process to be followed.

This lack of a strategic agenda on IW policy is in direct contrast to other countries, such as Russia.[36] Until the White House issues a cogent expression of national will on IW, it will not receive national recognition as a valid threat.

The second aspect of the IW threat is the nature of American society itself and how this has pervaded somewhat into the military environment. The United States, it is no surprise, is an open, trusting society. We have created an involuntary *glasnost* when it comes to information systems proliferation. As an illustration, once the two bombing incidents (mentioned above) passed, the American people went back to business as usual. We become complacent. The information systems we are obtaining welcome us to a new world of toys and opportunities, in many cases. The United States must develop ways to defend against IW attacks or face the same type of dilemma (but perhaps not the same degree) the Japanese people faced in August 1945 when President Truman ordered the atomic bombing of Hiroshima and Nagasaki. Had the Japanese government known of the destructive power that splitting the atom possessed, surely they would have developed civil defense measures or at least warnings for their own people. Today, America faces the same challenge in IW. We do not truly know the potential lethality that IW possesses. We will face another Hiroshima if we do not develop means to defend against IW attacks.

In the Joint arena, information technology promises great advantage to our already superior conventional military strength. The EXFOR's efforts at the NTC will prove to be a worthwhile investment in digitization. However, we must realize that technology, especially information technology, is a tool for the warfighter, not an end in itself. What makes this technology so great an addition to the warfighters array of systems is its ability to help the Joint Force Commander see and sense better, communicate with his forces faster, bring decisive firepower and maneuver to bear more accurately and economically, and achieve decisive victory -- in whatever format -- with fewer casualties and with less equipment loss. It will allow commanders to achieve what FM 100-6, Information Operations, calls "information dominance."[37] But behind the technology is the human element: take away the means of doing business and we are left with the source and the objective of all power: people.

The Joint Community must also learn what constitutes an IW attack. For example, cutting a transmission cable accidentally (as is often done in construction), is not necessarily an information attack. Whereas the cyber attack is often undetectable, cutting a cable is usually not. This is also why an IW attack is dangerous; you cannot see it, locate it, tell when it occurred or even if an attack occurred at all.

Another perspective that we often overlook is the fact that the United States is a unique society because it is nearly self-sufficient. It has many of the natural resources, technology, a relatively free and open working environment with two cooperative and friendly neighbors in Canada and Mexico. In many aspects the U.S. is able to determine its own destiny, as it has in the past through hard work, democratic ideals, and a market economy. But in an information warfare environment, no one country or people control information and the means to its use. Access is nearly unrestricted to so many of the systems which connect American society. For the first time, America may not be able to control its own destiny if and unless it can find the means to control the negative aspects of information warfare and information technology. This is why IW is so dangerous. Imagine, for instance a country or group that was able to obtain global information dominance, whatever that eventually means. The implications of knowing all that your adversaries especially were doing, thinking, planning are staggering. Information warfare could become a center of gravity.

The third component of the threat is inherent in the Information Age environment itself. Internetting and networking are two of the advantages of the technology of the Information Age. The proliferation of new and better ways to leverage that technology, however, has not brought with it the maturity to plan for the effective management of that technology. As a glaring example: few people have asked what will happen if the EXFOR digitization effort does not work. Key leaders and certainly the participants who have invested the past three years in this great experiment of integrating technology with advanced doctrinal concepts, certainly have assumed that it will be successful, albeit to differing degrees of success. Take, for another example, the American experience with the automobile. It was invented and put into production at the turn of this century and we are still killing ourselves by the thousands annually because we have not yet fully integrated automobile usage in our society. As a more basic example, what do you do when the power in your home goes out or your computer "crashes?" We have come to depend on technology for managing a large part of our lives. We must understand information technology development as we go along. We cannot develop management techniques after the means to use them are in every home or mounted on every combat vehicle on the battlefield.

The last component of the threat is the lack of a current conventional weapon threat. With the end of the Cold War and the collapse of the Soviet Union, the world is finding that all of those regional, ethnic, and nationalistic passions that were subordinated to the East-West power struggle were never really dead and they are now rising to the top of World consciousness. Information technology has risen to the top of this Post-Cold War world because it has such unlimited potential for both positive and negative reasons. With efforts to denuclearize former nuclear powers and the threat of large-scale nuclear or even conventional conflicts subsiding, the political focus is on regional conflicts. So, too, information technology is developing the hidden potential in information and in systems, in and of themselves, not as tools. This is a dangerous trend that if left unmanaged worldwide, could lead to an Information Age Pearl Harbor.

Conclusion

The Information Age holds great promise for technological achievement, for the betterment of all humans and for military users in particular. Some have theorized that with advanced information systems, such as stand-off weapons, long-range sensors, and unmanned aerial vehicles, the Joint arena might one day fight a war or conduct simultaneous attacks in depth or other operations "at a distance." The air war campaign of Desert Storm proved that with advanced technology we could obtain both air and information superiority and bring heavy damage to an enemy. What was needed to be decisive in that war, was the ability to combine the technology of air power with technology-driven ground forces. Coalition forces could not have achieved victory with personnel and equipment or information technology alone.

Americans have become dependent on information technology to the point that we find it is difficult to live without it. Our business transactions increasingly focus on electronic currency despite the fact that, as shown above, banks have suffered at the hands of hackers to those funds transfer systems. Force XXI's techno-Brigade is counting on technological innovations to drive Twenty-First Century tactics, techniques and procedures as well as doctrine, personnel, and logistics initiatives.

The United States and the Department of Defense are at a crossroads in information technology. As the Defense Science Board Task Force concluded:

> "There is a need for extraordinary action to deal with the present and emerging challenges of defending against possible information warfare attacks on facilities, information, information systems, and networks of the United States which would seriously affect the ability of the Department of Defense to carry out its assigned missions and functions. We have observed an increasing dependence on the Defense Information Infrastructure and increasing doctrinal assumptions regarding the continued availability of that infrastructure. This dependence and these assumptions are ingredients in a recipe for a national security disaster."[38]

This a valid argument. If TF XXI proves that indeed technology can be integrated successfully into combat operations, then the Department of Defense needs to adapt the lessons learned *BY THE*

OPFOR at NTC as examples of what automation can do to us when it is aimed at US Forces. While it is true that there is probably not a comprehensive threat to America's national security from a unified band of computer hackers, there is enough evidence to prove that there is an automation battle occurring in the Information environment.

Throughout history, when Man invented some new technology and discovered it could be used as a weapon of war, such as the bow and arrow, gunpowder, the railroad, and the like, the adversary against whom these were used had to quickly develop defenses or risk annihilation. New tactics, techniques and procedures had to soon follow, both in the way to use the weapon offensively and, conversely, in the means to defend against it. Man invented cavalry, for instance, as a means to fight massed infantry. Armies then developed the 14-foot pike to defend against persons on horseback. Subsequently, foot soldiers developed the compound bow and employed it effectively against pikemen. Armor's development then took place.

We are now at a point in history when the first "shots" in the information war have already been fired: hackings, denials of service, penetrations of Defense information systems. Are these being created as a reaction to or consequence of the development of information technologies? If countries are truly in an information "warfare" environment, the next manifestation is likely to be as a counter to the US advantage in information technology.

ENDNOTES

[1] ______, "Growing Threat," Aviation Week and Space Technology, Vol. 135, (November 25. 1991), 29.
[2] Thomas, Timothy L., "Deterring Information Warfare: A New Strategic Challenge," Parameters 26 (Winter 1996):: 81.
[3] Caires, Greg. "Reimer: EXFOR On Track For Upcoming Warfighting Experiment," Defense Daily, 19 December 1996, p. 442.
[4] Libicki, Martin C., What Is Information Warfare?, (Washington, DC: U.S. Government Printing Office), 1995. Those definitions are: C2W (taken from Joint Pub 3-13.1) - attacks on our ability to command and control deployed forces; IBW - what results when all sensors, emitters, and processors are fused into intelligence, reconnaissance, surveillance, target acquisition, damage assessment processes, i.e., the product of intelligence gathering systems for the warfighter; EW - attempts to disrupt the physical flow of electrons or cryptographic processes in electronic systems; PSYW - classical psychological warfare or information directed against the human mind or the will; hacker warfare - attacks on computer networks; EIW - described in two forms, information blockade (comparing information to trade, i.e. an information blockade would be like a trade embargo) or information imperialism (the assumption that competition in economic relations resembles war); and cyberwarfare - information attacks on virtual personae or groups.
[5] Ibid, p. 7.
[6] Ibid, p. x.
[7] Ibid, p. 53. Libicki claims, "It seems excessive, ..., to extract a threat to national security from what, until now, has been largely a high-tech version of car theft and joy-riding." What seems more the threat, here, is the *potential* for damage to information systems that these hackings have demonstrated, the fact that hackers *can* attack.
[8] This idea was presented in a briefing: "Defensive Information Warfare: From here to the end state," given by Joint Staff/J-6 representatives to an Army War College class on Information Warfare on 30 Jan 97. The philosophy of this statement is that technology is increasing so rapidly, hacking is becoming more sophisticated, we are still transitioning into the Information Age from the Industrial Age, and just beginning to understand the applications and implications of information technology and "warfare" in this sense. To try to pin down finite descriptions of uncertain, incomplete phenomenon is a futile exercise.
[9] Civilian and commercial discussions do not (and cannot) include the word warfare because it is an oxymoron: civilians do not conduct warfare. However, as shown at the beginning of this paper, there have been information warfare attacks against commercial, non-military systems and any computer-based system is susceptible to an information warfare "attack." What constitutes an "attack" will be discussed below.
[10] Joint Publication 3-13.1, p. GL-8. (Washington, DC: Joint Chiefs of Staff, February 1996). Additionally, information superiority is defined as "that degree of dominance in the information domain which permits the conduct of operations without effective opposition." (Ibid) (What form that opposition may take, e.g. conventional, nuclear, other information warfare techniques, is not named.)
[11] Department of Defense, "Report of the Defense Science Board Task Force on Information Warfare - Defense," (Washington, DC: Office of the Undersecretary of Defense for Acquisition and Technology, November 1996), p. 2-3.
[12] Wall Street Journal, 21 Oct 96, B11, cited in US Army Reserve Command (USARC) Bulletin 1-97, Jan 97, p. 8.
[13] Stern, 17 Oct 96, p. 124, cited in USArmy Reserve Command (USARC) Bulletin 1-97, Jan 97, p. 8-9.
[14] **AWACS** - Airborne Warning and Control System; **JSTARS** - Joint Surveillance Target Attack Radar System; **SBIR** - Space-Based Infrared Radar; **TARPS/ATARS** - Tactical Aerial Reconnaissance Pod System/Advanced Tactical Aerial Reconnaissance System; **MTI** - Moving Target Indicator; **REMBAS** - Remotely Monitored Battlefield Area Sensor System; **ISAR** - Inverse Synthetic Aperture Radar; **NVG** - Night Vision Goggles; **FDS** - Fixed Distribution System; **JDISS** - Joint Deployable Intelligence Support

System; **GCCS** - Global Command and Control System; **MILSTAR** - Military Strategic and Tactical Relay System; **JSIPS** - Joint Services Imagery Processing System; **DISN** - Defense Information Systems Network; **SABER** - Surface-to-Air Beam Rider; **C4I FTW** - Command, Control, Communications, Computers, and Intelligence For the Warfighter; **TIES** - Theater Information and Engagement System; **TADIL J** - Tactical Data Information Link - JTIDS; **TRAP** - Tactical Recovery of Aircraft and Personnel; **TACSAT** - tactical satellite; **MIDS** - Multifunctional Information Distribution System; **STEP** - Standard Tactical Entry Point; **SONET** - Synchronous Optical Network; **JMCIS** - Joint Maritime Command Information System; **Link-16** - subsystem of JTIDS; **DMS** - Defense Message System; **JTIDS** - Joint Tactical Information Distribution System; **SFW** - Sensor Fuzed Weapon; **JSOW** - Joint Standoff Weapon; **TLAM (blk III)** - Tomahawk Land Attack Missile, block III [version III]; **ATACS/BAT** - Advanced Tank Cannon System/Brilliant Anti-Armor Technology; **THAAD** - Theater High Altitude Air Defense; **SLAM** - Standoff Land Attack Missile; **CALCM** - Conventional Air-Launched Cruise Missile; **JDAM** - Joint Direct Attack Missile; **AGM-130** - Air-to-Ground Missile; **HARM** - High-Speed Anti-Radiation Missile; **LOSAT** - Low-Orbiting Satellite; **SADARM** - Sense and Destroy Armor; **AFTADS** -Advanced Field Artillery Tactical Data System

[15] Shalikashvili, John M., Pamphlet entitled Joint Vision 2010, (Washington, D.C.: Chairman of the Joint Chiefs of Staff, undated), p. 5. See also Reimer, Dennis J., Pamphlet entitled Army Vision 2010, (Washington, DC: Department of the Army, undated), p. 1, and Department of the Army, TRADOC PAM 525-5, Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century, (Fort Monroe, VA: U.S. Army Training and Doctrine Command, 1 Aug 94), p. 2-10 - called *Spectrum Supremacy*.

[16] National Defense University, Strategic Assessment 1996: Instruments of U.S. Power, (Washington, D.C.: National Defense University, 1996), p. 190.

[17] Dubrik, Jim, Info Paper: Status of the Quadrennial Defense Review (QDR) (C-8), 16 Jan 97, p. 4.

[18] "Info Warriors: Battling For Data Dominance in the Fifth Dimension," Airman, (September 1996), 27.

[19] Jimmy D. Ross, "Winning the Information War," Army, (February 1994), 27.

[20] Quoted in Airman, op cit, 28. Campden also stated that in the war, "an ounce of silicon in a computer may have had more effect than an a ton of uranium." (Ibid)

[21] "Information is the currency of victory on the battlefield," said former Army Chief of Staff General Gordon R. Sullivan (Joint Pub 3-13.1, op. cit., p. I-3). Gaining the advantage in information, according to Secretary of the Air Force Sheila Widnall," is becoming as critical as air and space superiority. The side that can capture the speed and power of the information revolution will have a tremendous advantage." (Sheila E. Widnall, speech to the Air Force Association National Symposium, Los Angeles, October 1995, in "Info Warriors Battle For Data Dominance in the Fifth Dimension," op. cit., 27.)

[22] Ross, op. cit., 28.

[23] I am indebted to classmate LTC(P) Karl Horst for this observation.

[24] Libicki, op. cit.

[25] US Army War College briefing to LTG Otto Guenther, Director, Information Systems for Command, Control, Communications, and Computers, 30 Jan 97. The conclusion: "only 1 of 250 successful attacks resulted in an active defensive response from the organizations: against which the attacks occurred. Also, key words such as *nuclear, weapons, Desert Shield,* and *Desert Storm* were most often targeted.

[26] _______ , "A New Worry: Terrorism in Cyberspace," Parade, September 29, 1996, p. 14.

[27] Lohr, "Ready, Aim, Zap: National Security Experts Plan for Wars Whose Targets and Weapons Are All Digital," New York Times, September 30, 1996, D1.

[28] George F. Stein, "Information Warfare," Airpower Journal (Spring 1995), 38-39.

[29] DSB Report, op. cit., ES-1.

[30] Lohr, op. cit., D-1.

[31] Paul Evancoe and Mark Bentley, "CVW - Computer Virus as a Weapon," Military Technology, May 1994, 40.

[32] William Clinton, A National Security Strategy of Engagement and Enlargement, (Washington, D.C.: The White House, Feb 96),

[33] In the section on enhancing our national security through active intelligence programs, the strategy includes "identifying emerging threats to modern information systems." Ibid, 25. On the next page, national security emergency preparedness includes the prevention of terrorism, the proliferation of weapons of mass destruction, and "threats to our information systems." (Ibid, 26.)

[34] The CIWG, created by Executive Order 13010 on 15 Jul 96, looks at concerns surrounding the protection of critical infrastructures such as telecommunications, electric power and transportation. The NTSAC, created by Executive Order 12382 in September 1982 and validated biennially, engages senior corporation executives from major carriers, information systems providers, electronics firms, and aerospace firms on matters regarding policies on national security and emergency preparedness telecommunications.

[35] Joint Chiefs of Staff, National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement, (Washington, D.C.: Joint Chiefs of Staff, 1995).

[36] Thomas, op. cit. One Russian theoretician stated: "From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not...Russia retains the right to use nuclear weapons first against the means and forces of information warfare and then against the aggressor state itself." V.I. Tsymbal, "Konseptsiya Informatsionnoy voyny" (Concept of Information Warfare), speech given at the Russian-U.S. conference on "Evolving Post-Cold War National Security Issues," Moscow 12-14 September 1995, p. 7, quoted in Thomas.

[37] Department of the Army, FM 100-6, Information Operations, (Washington, D.C.: Department of the Army, 27 Aug 96), 6-5.

[38] Defense Science Board Report, op. cit., cover letter.

BIBLIOGRAPHY

Bender, Bryan. "Troops in Bosnia Left Out of Information Loop, Analysis Finds." Defense Daily, 16 December 1996, p. 420.

Bender, Bryan. "U.S. Intelligence Sharing In Bosnia Unprecedented." Defense Daily, 10 October 1996, p. 61.

Caires, Greg. "Reimer: EXFOR On Track For Upcoming Warfighting Experiment." Defense Daily,19 December 1996, p. 442.

Cooper, Pat. " 'Automation...is Great.' " Air Force Times, 4 November 1996, p. 30.

Coughlin, Captain Sean, U.S. Naval Proceedings, Vol 118/11/1,077, p. 61.

Dubrik, Jim. Information Paper: Status of the Quadrennial Defense Review (QDR) (C-8), 16 Jan 97.

Evancoe, Paul and Mark Bentley. "CVW - Computer Virus As a Weapon," Military Technology (May 1994): 40-41.

Harknett, Richard J. "Information Warfare and Deterrence." Parameters 26 (Autumn 1996): 93- 107.

Hughes, David, ed."Aerobyte," Aviation Week and Space Technology, 19 February 1996, p.51.

Libicki, Martin C. What Is Information Warfare Washington: National Defense University, 1995.

Lohr, Steve. "Ready, Aim, Zap: National Security Experts Plan For Wars Whose Targets and Weapons Are All Digital." New York Times, 30 September 1996, 2.

Lykke, Arthur F., Jr. Military Strategy: Theory and Application. Carlisle Barracks, PA: USAWC, 1993.

Molander, Roger C., Andrew C. Riddile, and Peter A. Wilson. "Strategic Information Warfare: A New Face of War." Parameters 26 (Autumn 1996): 81-92.

National Defense University. Strategic Assessment 1996: Instruments of U.S. Power. Washington: National Defense University, 1996.

Paxton, Patrick. "Future Seizes Operations Other Than War." Army Times, 25 November 1996, p. 8.

Reimer, Dennis J. Army Vision 2010. Washington: Department of the Army, undated.

Rigby, MG Joe W. "Digitizing Force XXI: A Team Effort." Army (May 1995): 36-44.

Rohde, Commander. "What is Info Warfare." U.S. Naval Institute Proceedings, February 1996: 34.

Ross, Jimmy D. "Winning the Information War." Army 44 (February 1994): 26-32.

Sandberg, Jared. "U.S. Households With Internet Access Doubled to 14.7 Million in Past Year, Wall Street Journal, 21 Oct 96, B11.

Scales, BG Robert H., Jr., et al, Certain Victory: The US Army in the Gulf War. New York: Black Star Agency, 1993.

Schiesel, Seth. "Air Force Computer Invaded As Hackers Forge Web Page," New York Times, 31 December, 1996, p. D18.

Shalikashvili, John M. Joint Vision 2010. Washington: Chairman of the Joint Chiefs of Staff, undated.

Stein, George F. "Information Warfare." Airpower Journal (Spring 1995): 30-39.

The White House. A National Security Strategy of Engagement and Enlargement. Washington: The White House, 1996.

Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." Parameters 26 (Winter 1996-97): 81-91.

U.S. Department of the Army. Information Operations. FM 100-6. Washington: U.S. Department of the Army, 1996.

U.S. Department of the Army. Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Early Twenty-First Century. TRADOC PAM 525-5. Fort Monroe, VA: Training and Doctrine Command, 1 Aug 94.

U.S. Congress. Senate. Committee on Governmental Affairs. Permanent Subcommittee on Investigations. Prepared Testimony of Jim Christy, Air Force Investigator: Hearings on Security in Cyberspace. 105th Cong., 1st sess., 5 June 1996.

US Department of Defense, DoD Directive S-3600.1, Information Operations, (Washington, DC: 9 December 1996).

U.S. Department of Defense. Report of the Defense Science Board Task Force on Information Warfare - Defense. Washington: Office of the Undersecretary of Defense for Acquisition and Technology, 1996.

U.S. Joint Chiefs of Staff. Joint Doctrine For Command and Control Warfare (C2W). Washington: Joint Chiefs of Staff, 1996.

U.S. Joint Chiefs of Staff. National Military Strategy of the United States of America: A Strategy of Flexible and Selective Engagement. Washington: Joint Chiefs of Staff, 1995.

______. "A New Worry: Terrorism in Cyberspace." Parade (September 1996): 14.

______. "Cracker Attack Paralyzes Panix." Wall Street Journal, 12 September 1996, p. B1, quoted in US Army Reserve Command (USARC) Bulletin 12-96, (December): 7.

______. "Electronic Seal of Approval." Information Week, 5 August 1996, p. 22, quoted in US Army Reserve Command (USARC) Bulletin 11-96 (November 1996): 9.

______. "Government Tab For Century Date Change Could Reach $30 Billion." BNA Daily Report for Executives, 22 August 1996, p. A8, quoted in US Army Reserve Command (USARC) Bulletin 11-96 (November 1996): 9.

______. "Growing Pains on the Net." Business Week, 26 August 1996, p. 62, quoted in US Army Reserve Command (USARC) Bulletin 11-96 (November 1996): 9.

______. "Growing Threat," Aviation Week and Space Technology, 25 November 1991, p. 29.

______. "Info Oops!" Inside the Air Force, 25 October 1996, p. 1.

______. "Info Warriors: Battling For Data Dominance in the Fifth Dimension." Airman (September 1996): 26-31.

______. "Pentagon Needs New Vision," Defense News, 14-20 October, 1996, p. 58.

______. "System Cracker Got Recipe From Hacker Magazine," Wall Street Journal, 13 September 1996, p. B5, quoted in US Army Reserve Command (USARC) Bulletin 12-96 (December 1996): 7.

______. "Vandals At the Gates of the Internet," New York Times, 19 September 1996, C1, quoted in US Army Reserve Command (USARC) Bulletin 12-96 (December 1996): 7.

______. "Wired World Will 'Diminish National Sovereignty,' " BNA Daily Report for Executives, 6 September 1996, p. A14, quoted in US Army Reserve Command (USARC) Bulletin 11-96 (November 1996): 9.

______. Stern, 17 Oct 96, 124.